Docket No.: 50435-015

PATENT

2700

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

#29



In re Application of

Li GONG

Serial No.: 08/883,636 — Group Art Unit: 2132

Filed: June 26, 1997 — Examiner: D. Meislahn

For: LAYER-INDEPENDENT SECURITY FOR COMMUNICATION CHANNELS

## TRANSMITTAL OF APPEAL BRIEF

Commissioner for Patents
Washington, DC 20231

Sir:

Submitted herewith in triplicate is Appellant(s) Appeal Brief in support of the Notice of Appeal filed January 24, 2002. Please charge the Appeal Brief fee of $320.00 to Deposit Account 500417.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Wesley L. Strickland
Registration No. 44,363

600 13th Street, N.W.
Washington, DC 20005-3096
(202)756-8000 WLS:cac
Facsimile: (202)756-8087
**Date: March 25, 2002**

Docket No.: 50435-015 PATENT



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**



In re Application of :

Li GONG :

Serial No.: 08/883,636 : Group Art Unit: 2132

Filed: June 26, 1997 : Examiner: D. Meislahn

For: LAYER-INDEPENDENT SECURITY FOR COMMUNICATION CHANNELS

## APPEAL BRIEF

Commissioner for Patents
Washington, DC 20231

Sir:

This Brief is submitted pursuant to the Notice of Appeal submitted January 24, 2002 regarding the final rejection of claims 1-8, 13-20, 22-24, 26-32, 34 and 35 dated September 24, 2001.

## REAL PARTY IN INTEREST

Sun Microsystems, Inc. is the real party in interest in the pending application.



## RELATED APPEALS AND INTERFERENCES

No appeal or interference is known to Appellants that will affect or be directly affected by or have a bearing on the Board's decision in the pending appeal. There is a Petition For Review of A Director's Decision filed July 19, 2001 that is still pending

resolution.

## STATUS OF CLAIMS

Claims 1-8, 13-20, 22-24, 26-32, 34 and 35 remain pending. All the pending claims stand under final rejection, from which rejection, this appeal is taken. Claim 29 is not specifically addressed in the detailed treatment of the claims in the Final Office Action; however, the Office Action Summary identifies claim 29 as rejected and Appellants have prepared this Appeal Brief under the assumption that the Examiner's actual intentions with regard to claim 29 are reflected by the Summary Sheet.

## STATUS OF AMENDMENTS

None of the claims have been Amended after the Final Office Action dated September 24, 2001.

## SUMMARY OF INVENTION

The present invention provides layer-independent secure communications in a multi-layered communication network. In general, a communication channel or connection is first established between a first multi-layered network node and a second multi-layered network node. Then, a first stream is established between a first process, executing on the first node, and the communication channel. A second stream is then established between a second process, executing on the second node, and the communication channel. As the first process writes data to the first stream, the data is encrypted and when the encrypted data is read out of the second stream by the second

process, the data is decrypted.

There are several benefits achieved by the claimed invention. These are set forth, for example, on pages 2 and 3 of the specification. When the amount of information included in session is small, for example, when a session contains only a single message, then the overhead contributable to set up negotiation can adversely affect communications performance. This negative is overcome by the claimed invention. Further, some communication architectures do not include a session layer, which requires that a session layer be added to support session type security, further degrading performance. Layer specific encryption can avoid the overhead penalty associated with set up negotiation, but it has additional limitations. First, encryption and decryption must occur at the same corresponding layer on both the transmitting and receiving network nodes. The traditional techniques such as the simple key management for internet protocols (SKIP) and secure sockets layer (SSL) each require layer specific function calls. The result is that one application implementing security according to SKIP cannot interact with another application implementing security according to SSL. In addition, layer-specific encryption could be difficult to employ an object-oriented environments because of the inherent level of abstraction required. For example, some layers operate of databytes, which often is a much lower level than objects in an object oriented environment.

## ISSUES

The following issues are presented by this Appeal, whether the Examiner erred in:

a) rejecting claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(e) for anticipation by *Helwig et al.* (US Patent No. 5,793,749);

b) rejecting claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(b) for anticipation by *Schneier* (Applied Cryptography); and

c) rejecting claims 2, 3, 4, 6, 7, 8, 14, 15, 16, 18, 19, 22, 23, 26, 27, 30, 31, 34 and 35 under 35 USC §103 as unpatentable over either *Helwig et al.* or *Schneier.*

## GROUPING OF CLAIMS

Each claim is argued separately and each claim stands or falls independently of any other.

## ARGUMENT

### A. The Examiner erred in rejecting claims 1, 5, 13, 17, 20, 24, 28 and 32 as anticipated by Helwig et al.

The factual determination that *Helwig et al.* identically disclose the claimed inventions recited in claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(e) is erroneous given the differences between the claimed inventions and the system of *Helwig et al.* The portion of the specification of *Helwig et al.* relied upon by the Examiner refers to and describes Figure 3 and, more particularly, to a "pre-transmit process 68" within Figure 3. The whole purpose of that particular branch coming off of 66-Y (in which the pre-transmit process 68 is included) is to record a test message in memory.

The Examiner's rejection is predicated upon an inaccurate factual determination. The factual determination of lack of novelty under 35 USC §102 requires the identical disclosure in a single reference of each element of a claimed invention such that the

identically claimed invention is placed in possession of one having ordinary skill in the art. **Helfix, Ltd. v. Loc-Bloc, Ltd. 54 USPQ2d 1299 (Fed. Cir. 2000); TD Corporation v. Lydall, Inc. 159 F.3d. 534, 48 USPQ2d 1321 (Fed. Cir. 1998); Electro Medical Systems S.A. v. Coopoer Life Science, Inc., 34 F.3d. 1048, 32 USPQ2d 1017 (Fed. Cir. 1994).** There are significant differences between the invention recited in claims 1, 5, 13, 17, 20, 24, 28, and 32 and *Helwig et al.*'s system that contradict the factual determination that *Helwig et al.* identically describe the claimed invention within the meaning of 35 USC §102.

With respect to claim 1, there is no teaching or suggestion within *Helwig et al.* of:

a) establishing a communications channel in which there is then established "a first stream between the first process and the communication channel"; and

b) "establishing a second stream between the second process and the communication channel"; and

c) encrypting, independent of a transport protocol, data in response to the data being written to the first stream; and

d) decrypting, independent of the transport protocol, the encrypted data in response to the encrypted data being read form the second stream.

In addition to the features identified above with respect to claim 1, claim 5 recites a computer-readable medium, carrying code that when executed performs various functions. This requirement of claim 5 is not disclosed by *Helwig et al.*

In addition to the features identified above with respect to claim 1, claim 13 recites a computer data signal embodied on a carrier wave, representing instructions that when executed performs various functions. This requirement of claim 13 is not disclosed by *Helwig et al.*

With respect to claim 17, there is no teaching or suggestion within *Helwig et al.* of:

a) establishing a stream between a process and a communication channel; and

b) encrypting data independent of communication protocol layers in response to data being written to the stream.

With respect to claim 20, there is no teaching or suggestion in *Helwig et al.* of:

a) establishing a first stream from a first process to the communication channel; and

b) establishing a second stream from the communication channel to a second process.

In addition to the features identified above with respect to claim 20, claim 24 recites a computer-readable medium, carrying code that when executed performs various functions. This requirement of claim 24 is not disclosed by *Helwig et al.*

In addition to the features identified above with respect to claim 20, claim 28 recites a communications network performing the recited method steps. This requirement of claim 28 is not disclosed by *Helwig et al.*

In addition to the features identified above with respect to claim 20, claim 32 recites a computer data signal embodied on a carrier wave, representing instructions that when executed performs various functions. This requirement of claim 32 is not disclosed by *Helwig et al.*

The above argued differences between the claimed inventions and the system of *Helwig et al.* undermine the factual determination that *Helwig et al.* identically describe the claimed inventions within the meaning of 35 USC §102. **Kolster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 230 USPQ 81 (Fed. Cir. 1986). Thus, the Examiner has failed to establish a prima facie case of anticipation.** Appellants, therefore, respectfully submit that each the imposed rejection of claims 1, 5, 13, 17, 20, 24, 28 and

32 under 35 USC §102 for lack of novelty, as evidenced by *Helwig et al.*, are independently factually erroneous.

**B. The Examiner erred in rejecting claims 1, 5, 13, 17, 20, 24, 28 and 32 as anticipated by Schneier.**

The Examiner erred in rejecting claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(b) as anticipated by *Schneier* (Applied Cryptography). The factual determination that *Schneier* identically disclose the claimed inventions recited in claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(b) is erroneous given the differences between the claimed inventions and the system of *Schneier*. *Schneier* describes an XOR encryption process, known as a stream cipher, with its corresponding decryption process. With respect to all the claims, this discussion of a ciphering model by *Schneier* does not disclose (or even suggest) establishment of a communications channel followed by establishing a stream between a process and the channel and another stream from the channel to an output process. Thus, the Examiner has failed to establish a *prima facie* case of anticipation.

With respect to claim 1, there is no teaching or suggestion within *Schneier* of:

a) establishing a communications channel in which there is then established "a first stream between the first process and the communication channel"; and

b) "establishing a second stream between the second process and the communication channel"; and

c) encrypting, independent of a transport protocol, data <u>in response to the data being written to the first stream</u>; and

d) decrypting, independent of the transport protocol, the encrypted data <u>in</u>

response to the encrypted data being read form the second stream.

In addition to the features identified above with respect to claim 1, claim 5 recites a computer-readable medium, carrying code that when executed performs various functions. This requirement of claim 5 is not disclosed by *Schneier*

In addition to the features identified above with respect to claim 1, claim 13 recites a computer data signal embodied on a carrier wave, representing instructions that when executed performs various functions. This requirement of claim 13 is not disclosed by *Schneier*

With respect to claim 17, there is no teaching or suggestion within *Schneier* of:

a) establishing a stream between a process and a communication channel; and

b) encrypting data independent of communication protocol layers in response to data being written to the stream.

With respect to claim 20, there is no teaching or suggestion in *Schneier* of:

a) establishing a first stream from a first process to the communication channel; and

b) establishing a second stream from the communication channel to a second process.

In addition to the features identified above with respect to claim 20, claim 24 recites a computer-readable medium, carrying code that when executed performs various functions. This requirement of claim 24 is not disclosed by *Schneier*.

In addition to the features identified above with respect to claim 20, claim 28 recites a communications network performing the recited method steps. This requirement of claim 28 is not disclosed by *Schneier*

In addition to the features identified above with respect to claim 20, claim 32

recites a computer data signal embodied on a carrier wave, representing instructions that when executed performs various functions. This requirement of claim 32 is not disclosed by *Schneier*

The above argued differences between the claimed inventions and the system of *Schneier* undermine the factual determination that *Schneier* identically describe the claimed inventions within the meaning of 35 USC §102. **Kolster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 230 USPQ 81 (Fed. Cir. 1986).**

**Thus, the Examiner has failed to establish a prima facie case of anticipation.** Appellants, therefore, respectfully submit that each the imposed rejection of claims 1, 5, 13, 17, 20, 24, 28 and 32 under 35 USC §102 for lack of novelty, as evidenced by *Schneier*, are independently factually erroneous.

**C. The factual determination that either *Helwig et al.* or *Schneier* identically disclose (or even suggest) a "stream" as meant and recited in <u>any</u> of the present claims is erroneous when the appropriate disclosures are considered as a whole and interpreted with internal consistency and from the perspective of one of ordinary skill.**

Neither *Helwig et al.* nor *Schneier* teach or suggest the use of a "stream" as that term was used or applied in the specification and claims of the present application.

*<u>Helwig et al.</u>:*

*Helwig et al.* does refer to a "data stream" However, the use of similar <u>sounding</u> terms is not necessarily the same as using terms that <u>mean</u> the same thing. Therefore, the mere use of similar sounding terms does not end the inquiry into whether a reference can be considered as identically disclosing the same subject matter. The meaning of "data streams" in *Helwig et al.* is interpreted in the context of that specification and within

*Helwig et al.* the "data streams" are a series of bits output from a vocoder and are used as a description of the data's particular physical format.

In contrast to the interpretation as meant by *Helwig et al.*, the present claim term "stream" is to be interpreted in light of the claim language, the specification, and the prosecution history; and the interpretation proceeds from the vantage point of one skilled in the art. **Atlantic Thermoplastics Co., Inc. v. Faytex Corp., 970 F.2d 834, 23 USPQ2d 1481 (Fed. Cir. 1992); Haynes International, Inc. v. Jessop Steel Co., 8 F.3d 1573, 28 USPQ2d 1652 (Fed. Cir. 1993).** Ultimately, claim language is construed according to the standard of what those words would have meant to one skilled in the art as of the application date. **Weiner v. NEC Electronics, Inc., 102 F.3d 534, 41 USPQ2d 1023 (Fed. Cir. 1996).**

It is important to interpret the phrase "stream" within the claims in a way which is consistent with the specification, rather than at odds to it. For example, one would obviously not interpret "stream" in the context of this application as referring to a flow of water down a mountain side. On page 4 of the specification, beginning line 9, the application introduces a "stream" as an abstraction which refers to the transfer or "flow" of data, in any format, from a single source, to a single destination. Let us consider the following example in the context of Figure 1 of the application. Let us assume that process 108 is an MPEG2 transmission process. It may generate a plurality of "streams", such as a left channel audio, a right channel audio, a video, a closed-captioned stream, and a control channel stream. When the MPEG2 transmission process 108 desires to send information to process 110, which, in this example, is an MPEG2 display process, a communications channel would be set up between node 108 and node 104 then, the individual streams

would be applied to the communications channel for transmission to the node 104. Note that the communication channel from the process 108 goes through all of the layers shown in Figure 1 of each protocol stack, namely the application layer, presentation layer, session layer, transport layer, network layer, datalink layer, and physical layer before going across the transmission medium to the other node and then passing through the same layers as an inverse order. It is known in the art to apply layer specific encryption at any of the layers of the OSI reference model shown in Figure 1.

If the invention of claim 1 were applied to a communication system which corresponded to the OSI reference model, first, communications would be established between the first network node and the second network node. The request for connection would come from the process 108 to the application layer and appropriately process through the layers until a connection is set up to node 104. Once that is done, a first stream, say, for example, an MPEG control channel stream is established between the first process 108 and the communications channel which begins at application layer 118. At the other end, a stream would be established between the application layer 128 of node 104 and the process 110 for the MPEG control channel data. As set forth in limitation d) of claim 1, in response to data being written to the first stream [from process 108] the data is encrypted to generate encrypted data which is then applied to the application layer 118. The encryption is performed independently of any of the layers of the communications protocol stack. Note that in the example of MPEG2, encryption can be applied selectively to the streams rather than to everything that is transmitted over the communications channel. In OSI reference model, the layer normally responsible for encryption is the presentation layer while the application layer, 118, handles the interface between the

software involved with the process 108 and the communications channel.

One limitation of claim 1 states "in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover the decrypted data."

As used within the present application, "stream" is an abstraction, which has properties beyond merely being a string of binary digits. "Streams", as would be understood by a skilled software practitioner, are defined in object oriented languages such as Java and have a whole set of associated properties which distinguish them from a flow of water down the mountain side and which also distinguish them from simply an arbitrary string of binary 1's and 0's.

*Schneier*:

With regards to *Schneier*, the referenced portion (Section 9.4) of his book **Applied Cryptography** describes a cipher model known as "Stream Ciphers". In particular, the Examiner relies of Figure 9.6 as anticipating the present claims. So, similar to Helwig et. al., *Schneier* also uses a similar sounding term -- "stream cipher"; but, once again, the inquiry is not whether similar sounding terms are being used but whether the terms being used convey an identical disclosure of subject matter as required under 35 USC §102.

The following information from **Ritter's Crypto Glossary and Dictionary of Technical Cryptography** (Current Edition: 2002 Feb 18, which can be found at, for example, http://www.ciphersbyritter.com/GLOSSARY.HTM)provides a helpful context for evaluating the disclosure of *Schneier*.

The glossary has a heading of "Cipher Taxonomy" which includes the following

definitions:

> **BLOCK CIPHER**
> A block cipher requires the accumulation of some amount of data or multiple data elements for ciphering to complete. (Sometimes stream ciphers accumulate data for convenience, as in cylinder ciphers, which nevertheless logically cipher each character independently.)
>
> **STREAM CIPHER**
> A stream cipher does not need to accumulate some amount of data or multiple data elements for ciphering to complete. (Since we define only two main "types" of cipher, a stream cipher is the opposite of a block cipher and vise versa. It is extremely important that the definitions for block and stream ciphering enclose the universe of all possible ciphers.) A stream cipher has the ability to transform individual elements one-by-one. The actual transformation usually is a block transformation, and may be repeated with the same or different keying.

A later heading in this Glossary that relates to a "Stream Cipher" further agrees with the specific XOR implementation of *Schneier* by describing a stream cipher as:

> a cipher which directly handles messages of arbitrary size by ciphering individual data elements, such as bits or bytes or characters. Conventionally, some form of keyed random number generator is used to produce a confusion sequence or running key. That sequence is then combined with plaintext data by exclusive-OR to produce ciphertext. Enciphering individual characters allows ciphering to begin immediately, avoiding the need to accumulate a full block of data before ciphering, as is necessary in a conventional block cipher. But note that a stream cipher can be seen as an operating mode, a "streaming" of a tiny block transformation. Stream ciphers can be called "combiner-style" ciphers. Also see: a cipher taxonomy.

Appellants urge that the high-level discussion of a stream ciphering model by *Schneier* does not provide the requisite identical disclosure of the "stream" abstraction as intended and used in the present specification and claims.

Thus, the Examiner has failed to establish a *prima facie* case of anticipation of the

claims when the claims, *Schneier* and *Helwig et al.* are all properly interpreted, because such an interpretation reveals that neither of the references identically disclose the "stream" recited in the claims.

**D. The Examiner erred in rejecting claims 3, 4, 7, 8, 15, 16, 18, 19, 22, 23, 26, 27, 29, 30, 31, 34, and 35 as unpatentable over either Helwig et al. or Schneier.**

Claims 3, 4, 7, 8, 15, 16, 18, 19, 22, 23, 26, 27 [and 29], 30, 31, 34 and 35 are not obvious over either *Helwig et al.* or *Schneier* because neither of these references teach or other wise suggest a Java-based stream or communication channel and, thus, the Examiner did not discharge the initial burden of establishing a prima facie basis to deny patentability to the claimed invention under 35 USC §103.

In applying these references to the claims, the Examiner states:

> "They do not say that the communication channels or data streams are Java-based. Official notice is taken that it is old and well-known that Java is intended for networked/distributed environments and enables the construction of virus-free, tamper-free systems. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to base the systems of *Schneier* or *Helwig et al.*, all of which are networked or distributed environments, on Java, as is known in the art. This would enable the implementation of a virus-free, tamper-free system."

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision always rests upon the Examiner. **In re Mayne, 41 USPQ2d 1451 (Fed .Cir. 1997); In re Deuel, 34 USPQ2d 1210 (Fed. Cir. 1995); In re Bell, 26 USPQ2d 1529 (Fed. Cir. 1993); In re Oetiker, 24 USPQ2d 1443 (Fed. Cir. 1992).** In rejecting a claim under 35 U.S.C. § 103, the Examiner is required to provide a factual basis to support the obviousness conclusion. **In re Warner, 154 USPQ 173 (CCPA 1967); In re Lunsford, 148 USPQ 721 (CCPA 1966); In re Freed,**

**165 USPQ 570 (CCPA 1970).** The Examiner is required to show that all the claim limitations are taught or suggested by the references along with some motivation to combine the teachings of the references. **In re Royka, 180 USPQ 580 (CCPA 1974); In re Wilson, 165 USPQ 494 (CCPA 1970).**

In addition, it has been repeatedly held by the Court of Appeals for the Federal Circuit that in order to establish the requisite realistic motivation, the Examiner must make "clear and particular" factual findings as to a specific understanding or specific technological principle which would have realistically impelled one having ordinary skill in the art to modify a particular prior art device (the device of either *Schneier* or *Helwig et al.*) to arrive at the claimed invention based upon facts--not generalizations. **Ruiz v. A.B. Chance Co., 234 F.2d 654, 57 USPQ2d 1161 (Fed. Cir. 2000); Ecolochem Inc. v. Southern California Edison, Co. 227 F.3d 361, 56 USPQ2d 1065 (Fed. Cir. 2000); In re Kotzab, 217 F.3d 1365, 55 USPQ 1313 (Fed. Cir. 2000); In re Dembiczak, 175 F.3d 994, 50 USPQ2d 1614 (Fed. Cir. 1999).** Moreover, the Examiner is required to explain **why** one having ordinary skill in the art would have been realistically led to modify the devices of either *Schneier* or *Helwig et al.* to arrive at the claimed invention. **Ecolochem Inc. v. Southern California Edison, Co. supra.; In re Rouffet, 149 F.3d 1350, 47 USPQ2d 1453 (Fed. Cir. 1998).** Significantly, the requisite motivation must be undertaken with a reasonably expectation of successfully achieving the objective of either *Schneier* or *Helwig et al.* **In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).**

Appellant would heavily rely upon the legal tenet that regardless of what the Examiner perceives as the source of motivation in the prior art, the Examiner must

provide "a convincing discussion of the specific sources of the motivation to combine the prior art references...". **Ecolochem Inc. v. Southern California Edison, Co. 227 F.3d 1361, 56 USPQ2d 1065 (Fed. Cir. 2000)**. This basis legal tenet was recently enforced by the Court of Appeals for the Federal Circuit in **In re Lee ____F.3d ____, 61USPQ2d 1430 (Fed. Cir. 2002)**, wherein the Court emphasized that the motivational element is a factual question which requires substantial evidence--not conclusory statements.

Appellants continue to insist that the range and content of the Examiner's Official Notice is factually and legally erroneous. But, assuming for the sake of argument that the Official Notice was effective for what the Examiner asserts, Appellants urge that the requirements of 35 USC §103 have still not been satisfied. The Examiner has failed to provide a cogent explanation of why one of ordinary skill would have been motivated to modify the message storing device of to *Helwig et al.* to add, for example, the complexity, additional hardware and cost of Java processing capability in the first place. Additionally, the Examiner has failed to provide a cogent explanation of why one of ordinary skill would have been motivated to augment the general discussion of enciphering and deciphering models by *Schneier* to specifically involve Java and Java streams. The Examiner states that Java "enables construction of virus-free, tamper-free systems". This type of generalization about technology is exactly the danger of which the courts have repeatedly warned against and the type of reasoning which the courts have repeatedly found erroneous. The establishment of a prima facie case of obviousness must factually explain why one of ordinary skill would have been motivated to combine specific teachings, in a specific way in order to arrive at a specific invention.

The Examiner's Official Notice (even if true) that Java might have use in tamper-free systems, is not a factual explanation of why a skilled artisan would have found it obvious to modify the specific systems taught by *Schneier* or *Helwig et al.* with some reasonable expectation of success.

If the Examiner were to implement the *Schneier* or *Helwig et al.* systems, using Java streams and Java secure channels, it would still not result in the claimed invention. In fact, if the phrases "communication channel" and "stream" as used in each of the references are interpreted to be a "Java stream" and "Java secure communication channel," the interpretation of the references as applied to the independent claims would have to change so dramatically as to show their inapplicability under 35 USC §102.

Appellants urge that the Examiner committed clear factual and legal errors. Specifically, without the benefit of any facts, the Examiner expanded the teachings of the applied references to whatever level he needed in order to combine them, relying only upon his "official notice" ability, in complete violation of **Ex parte Stern, 13 USPQ2d 1379 (BPAI 1987).**

Appellants recognize that the specific limitations recited in the different "families" of dependent claims appear to be very similar. However, as the patentability of each of the independent claims was separately argued, Appellants wish to stress that the dependent claims also stand or fall individually and are not being grouped together.

With respect to claim 3, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 3 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 4, the claim recites a first Java stream, a second Java stream,

a third Java stream, and a Java secure channel. These requirements of claim 4 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 7, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 7 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 8, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 8 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 15, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 15 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 16, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 16 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 18, the claim recites a first Java stream and a Java secure channel. These requirements of claim 18 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 19, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 19 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 22, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 22 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 23, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 23 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 26, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 26 are not disclosedor suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 27, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 27 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 29, the claim recites that the encryption of the first stream and the decryption of the second stream is specific to a communication protocol layer. This requirement of claim 29 is not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 30, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 30 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 31, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 31 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 34, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 34 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 35, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 35 are not

disclosed or suggested by either *Helwig et al.* or *Schneier.*

The above argued differences between the claimed inventions and the system of *Helwig et al.* and *Schneier* undermine the factual determination that *Helwig et al.* and *Schneier* provide a prima facie case of obviousness within the meaning of 35 USC §103 of claims 3, 4, 7, 8, 15, 16, 18, 19, 22, 23, 26, 27, 30, 31, 34 and 35

**E. The Examiner erred in rejecting claims 2, 6, and 14 as unpatentable over either Helwig et al. or Schneier.**

Claims 2, 6, and 14 are not obvious over either *Helwig et al.* or *Schneier* because neither of these references teach or other wise suggest performing communication protocol layer specific encryption or decryption of the data and, thus, the Examiner did not discharge the initial burden of establishing a prima facie basis to deny patentability to the claimed invention under 35 USC §103.

In rejecting these claims, the Examiner asserts that if some encryption is good, then more encryption is better. Appellants admit that some liberty was taken with paraphrasing the Examiner's comments; however, if read carefully, his assertions really do not say anything more than the above generalization. As stated previously, the Examiner must make "clear and particular" factual findings as to a specific understanding or specific technological principle which would have realistically impelled one having ordinary skill in the art to modify a particular prior art device (the device of either *Schneier* or *Helwig et al.*) to arrive at the claimed invention based upon facts--not generalizations.

Each of claims 2, 6 and 14 require more than simply a second encryption step. The claims recite that the encryption being performed be "a communication protocol

layer specific encryption." The Examiner has not explained why a skilled artisan, with either *Schneier* or *Helwig et al.* in hand, would have found it obvious to add to the respective systems a communication layer protocol specific encryption. *Schneier* does not disclose a stream cipher in the context of networked nodes communicating over a channel and *Helwig et al.* is concerned about storing a message, not with secure communications. Additionally, *Helwig et al.* discusses the need for responsiveness in their system and one skilled in the art would not have adversely impacted performance in such a system by adding another layer of encryption processing. Accordingly, the Examiner's generalization might indicate that employing multiple layers of encryption was known and even that protocol specific encryption was known. However, these conclusions fall far short of establishing a prima facie case of obviousness under 35 USC §103. The Examiner has failed to provide a fact-based rationale why one of ordinary skill would have been motivated to modify specifically *Schneier* or *Helwig et al.* with a second encryption/decryption step and why that skilled artisan would have performed the encryption/decryption as being protocol layer specific.

The lack of a fact-based explanation for expanding the teachings of *Helwig et al.* and *Schneier* undermine the factual determination that *Helwig et al.* and *Schneier* provide a prima facie case of obviousness within the meaning of 35 USC §103 of claims 2, 6, and 14.

**F. Claims 2, 3, 4, 6, 7, 8, 14, 15, 16, 18, 19, 22, 23, 26, 27 [and 29], 30, 31, 34 and 35 are not obvious over either *Helwig et al.* or *Schneier* because neither of these references anticipate the respective independent claims from which these claims depend and, thus, the Examiner did not discharge the initial burden of establishing a prima facie basis to deny patentability to the claimed invention under 35 USC §103.**

In rejecting the dependent claims, the Examiner relies on either *Helwig et al.* or *Schneier* as applied to the independent claims and then asserts, through "Official Notice" that the specific features in the dependent claims are well-known.

As argued above, neither of the applied references disclose all the features of the independent claims -- features which are incorporated into respective dependent claims. Accordingly, for the reasons presented above, with regard to the independent claims, neither reference discloses or suggests every feature recited in the dependent claims.

Neither *Schneier* nor *Helwig et al.*, therefore, provide the factual basis needed to properly establish a prima facie case of obviousness under 35 USC §103.

## CONCLUSION

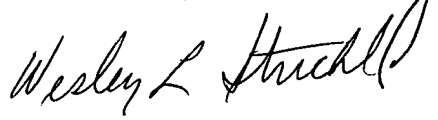
For the reasons advanced above, the Examiner's factual determination that *Schneier* identically describes the claimed inventions of claims 1, 5, 13, 17, 20, 24, 28 and 32, within the meaning of 35 USC §102, is erroneous. For the reasons advanced above, the Examiner's factual determination that *Helwig et al.* identically describe the claimed inventions of claims 1, 5, 13, 17, 20, 24, 28 and 32, within the meaning of 35 USC §102, is erroneous. Appellants, therefore, respectfully solicit the Honorable Board to **reverse** each of the Examiner's rejections.

For the reasons advanced above, Appellants submit that the Examiner did not establish a *prima facie* basis to deny patentability to any of the claims on Appeal under 35 USC §103. Appellants, therefore, respectfully solicit the Honorable Board to **reverse** each of the Examiner's rejections under 35 USC §103.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-0417 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Wesley L. Strickland
Registration No. 44,363

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 WLS:cac
**Date: March 25, 2002**
Facsimile: (202) 756-8087

APPENDIX

1. (Twice Amended) A method for providing communication protocol layer independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, wherein the first network node and the second network node each support at least one common communication protocol layer, the method comprising the steps of:

establishing a communication channel between the first network node and the second network node;

establishing a first stream between the first process and the communication channel;

establishing a second stream between the second process and the communication channel;

in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node;

causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of

the encrypted data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node.

2. (Thrice Amended) The method of Claim 1, further including the steps of

performing a communication protocol layer specific encryption of the data on the first network node, and

performing a communication protocol layer specific decryption of the data on the second network node.

3. The method of Claim 1, wherein the communication channel is a Java secure channel,

wherein the first stream is a first Java stream,

wherein the second stream is a second Java stream,

wherein the step of establishing a communication channel between the first and second network nodes further comprises the step of establishing a Java secure channel between the first and second network nodes,

wherein the step of establishing a first stream between the first process and the communication channel further comprises the step of establishing a first Java stream between the first process and the Java secure channel, and

wherein the step of establishing a second stream between the second process and the communication channel further comprises the step of establishing a second Java stream between the second process and the Java secure channel.

4. (Twice Amended) The method of Claim 1, wherein the communication channel is a Java secure channel, wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the method further comprises the step of connecting the Java secure channel to a third Java stream, and

wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

5. (Twice Amended) A computer-readable medium carrying one or more sequences of one or more instructions for providing communication protocol layer independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, wherein the first network node and the second network node each support at least one common communication protocol layer, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

establishing a communication channel between the first network node and the second network node;

establishing a first stream between the first process and the communication channel;

establishing a second stream between the second process and the communication channel;

in response to the data being written to the first stream, encrypting the data to

generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node;

causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node.

6. (Twice Amended) The computer-readable medium of Claim 5, wherein the computer-readable medium further includes instructions for performing the steps of

performing a communication protocol layer specific encryption of the data on the first network node, and

performing a communication protocol layer specific decryption of the data on the second network node.

7. The computer-readable medium of Claim 5, wherein the first stream is a first Java stream,

wherein the second stream is a second Java stream,

wherein the step of establishing a communication channel between the first and

second network nodes further comprises the step of establishing a Java secure channel between the first and second network nodes,

wherein the step of establishing a first stream between the first process and the communication channel further comprises the step of establishing a first Java stream between the first process and the Java secure channel, and

wherein the step of establishing a second stream between the second process and the communication channel further comprises the step of establishing a second Java stream between the second process and the Java secure channel.

8. (Amended) The computer-readable medium of Claim 5, wherein the communication channel is a Java secure channel,

wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the computer-readable medium further includes instructions for connecting the Java secure channel to a third Java stream, and

wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

13. (Twice Amended) A computer data signal embodied in a carrier wave and representing sequences of instruction which, when executed by one or more processors, provide communication protocol layer independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, according to at least one common communication protocol layer

supported by the first and second network nodes, by performing the steps of:

establishing a communication channel between the first network node and the second network node;

establishing a first stream between the first process and the communication channel;

establishing a second stream between the second process and the communication channel;

in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node;

causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node.

14. (Twice Amended) The computer data signal of Claim 13, wherein the computer sequence of instructions further includes instructions for performing the steps of

performing a communication protocol layer specific encryption of the data on the first network node, and

performing a communication protocol layer specific decryption of the data on the second network node.

15. The computer data signal of Claim 13, wherein the first stream is a first Java stream,

wherein the second stream is a second Java stream,

wherein the step of establishing a communication channel between the first and second network nodes further comprises the step of establishing a Java secure channel between the first and second network nodes,

wherein the step of establishing a first stream between the first process and the communication channel further comprises the step of establishing a first Java stream between the first process and the Java secure channel,

wherein the step of establishing a second stream between the second process and the communication channel further comprises the step of establishing a second Java stream between the second process and the Java secure channel.

16. (Amended) The computer data signal of Claim 13, wherein the communication channel is a Java secure channel,

wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the computer sequence of instructions further includes instructions for

connecting the Java secure channel to a third Java stream, and

wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

17. (Amended) A method for providing communication protocol layer independent security for data transmitted by a process executing on a network node, the method comprising the steps of:

a) establishing a stream between the process and a communication channel; and

b) in response to the data being written to the stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data on the communication channel.

18. (Amended) The method of Claim 17, wherein the communication channel is a Java secure channel,

wherein the stream is a first Java stream, and

wherein the step of establishing a stream between the process and the communication channel further comprises the step of establishing a Java stream between the process and the Java secure channel.

19. (Amended) The method of Claim 17, wherein the communication channel is a Java secure channel, wherein the stream is a Java stream,

wherein the method further comprises the step of connecting the Java secure channel to a second Java stream, and

wherein the second Java stream provides for the transmission of data according to a specific communication protocol layer.

20. (Amended) A method for providing communication protocol-independent security for data transmitted between a first node and a second node, the method comprising the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel after the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process after the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

22. (Amended) The method of claim 20, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node

and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

23. (Amended) The method of claim 20, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream;

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

24. (Amended) A computer-readable medium carrying one or more sequences of one or more instructions for providing communication protocol-layer independent security for data transmitted between a first node and a second node, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel after the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process after the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

26. (Amended) The computer-readable medium of claim 24, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

27. The method of claim 24, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

28. (Amended) A communications network providing communication protocol-independent security for data transmitted between a first node and a second node, the communication network performing the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel after the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process after the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

29. The communication network of claim 28, wherein the encryption of the first stream and the decryption of the second stream is specific to a communication protocol layer.

30. (Amended) The communication network of claim 28, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

31. The communication network of claim 28, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

32. (Amended) A computer data signal embodied in a carrier wave and representing sequences of instructions which, when executed by one or more processor, provide communication protocol-independent security for data transmitted between a

first node and a second node, by performing the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel after the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process after the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

34. (Amended) The computer data signal of claim 32, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

35. The computer data signal of claim 32, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

Docket No.: 50435-015 PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | | |
|---|---|---|
| In re Application of | : | |
| Li GONG | : | |
| Serial No.: 08/883,636 | : | Group Art Unit: 2132 |
| Filed: June 26, 1997 | : | Examiner: D. Meislahn |

For: LAYER-INDEPENDENT SECURITY FOR COMMUNICATION CHANNELS

## APPEAL BRIEF

Commissioner for Patents
Washington, DC 20231

Sir:

This Brief is submitted pursuant to the Notice of Appeal submitted January 24, 2002 regarding the final rejection of claims 1-8, 13-20, 22-24, 26-32, 34 and 35 dated September 24, 2001.

## REAL PARTY IN INTEREST

Sun Microsystems, Inc. is the real party in interest in the pending application.

## RELATED APPEALS AND INTERFERENCES

No appeal or interference is known to Appellants that will affect or be directly affected by or have a bearing on the Board's decision in the pending appeal. There is a Petition For Review of A Director's Decision filed July 19, 2001 that is still pending

resolution.

## STATUS OF CLAIMS

Claims 1-8, 13-20, 22-24, 26-32, 34 and 35 remain pending. All the pending claims stand under final rejection, from which rejection, this appeal is taken. Claim 29 is not specifically addressed in the detailed treatment of the claims in the Final Office Action; however, the Office Action Summary identifies claim 29 as rejected and Appellants have prepared this Appeal Brief under the assumption that the Examiner's actual intentions with regard to claim 29 are reflected by the Summary Sheet.

## STATUS OF AMENDMENTS

None of the claims have been Amended after the Final Office Action dated September 24, 2001.

## SUMMARY OF INVENTION

The present invention provides layer-independent secure communications in a multi-layered communication network. In general, a communication channel or connection is first established between a first multi-layered network node and a second multi-layered network node. Then, a first stream is established between a first process, executing on the first node, and the communication channel. A second stream is then established between a second process, executing on the second node, and the communication channel. As the first process writes data to the first stream, the data is encrypted and when the encrypted data is read out of the second stream by the second

process, the data is decrypted.

There are several benefits achieved by the claimed invention. These are set forth, for example, on pages 2 and 3 of the specification. When the amount of information included in session is small, for example, when a session contains only a single message, then the overhead contributable to set up negotiation can adversely affect communications performance. This negative is overcome by the claimed invention. Further, some communication architectures do not include a session layer, which requires that a session layer be added to support session type security, further degrading performance. Layer specific encryption can avoid the overhead penalty associated with set up negotiation, but it has additional limitations. First, encryption and decryption must occur at the same corresponding layer on both the transmitting and receiving network nodes. The traditional techniques such as the simple key management for internet protocols (SKIP) and secure sockets layer (SSL) each require layer specific function calls. The result is that one application implementing security according to SKIP cannot interact with another application implementing security according to SSL. In addition, layer-specific encryption could be difficult to employ an object-oriented environments because of the inherent level of abstraction required. For example, some layers operate of databytes, which often is a much lower level than objects in an object oriented environment.

## ISSUES

The following issues are presented by this Appeal, whether the Examiner erred in:

a) rejecting claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(e) for anticipation by *Helwig et al.* (US Patent No. 5,793,749);

b) rejecting claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(b) for anticipation by *Schneier* (Applied Cryptography); and

c) rejecting claims 2, 3, 4, 6, 7, 8, 14, 15, 16, 18, 19, 22, 23, 26, 27, 30, 31, 34 and 35 under 35 USC §103 as unpatentable over either *Helwig et al.* or *Schneier.*

## GROUPING OF CLAIMS

Each claim is argued separately and each claim stands or falls independently of any other.

## ARGUMENT

### A. The Examiner erred in rejecting claims 1, 5, 13, 17, 20, 24, 28 and 32 as anticipated by Helwig et al.

The factual determination that *Helwig et al.* identically disclose the claimed inventions recited in claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(e) is erroneous given the differences between the claimed inventions and the system of *Helwig et al.* The portion of the specification of *Helwig et al.* relied upon by the Examiner refers to and describes Figure 3 and, more particularly, to a "pre-transmit process 68" within Figure 3. The whole purpose of that particular branch coming off of 66-Y (in which the pre-transmit process 68 is included) is to record a test message in memory.

The Examiner's rejection is predicated upon an inaccurate factual determination. The factual determination of lack of novelty under 35 USC §102 requires the identical disclosure in a single reference of each element of a claimed invention such that the

identically claimed invention is placed in possession of one having ordinary skill in the art. **Helfix, Ltd. v. Loc-Bloc, Ltd. 54 USPQ2d 1299 (Fed. Cir. 2000); TD Corporation v. Lydall, Inc. 159 F.3d. 534, 48 USPQ2d 1321 (Fed. Cir. 1998); Electro Medical Systems S.A. v. Coopoer Life Science, Inc., 34 F.3d. 1048, 32 USPQ2d 1017 (Fed. Cir. 1994).** There are significant differences between the invention recited in claims 1, 5, 13, 17, 20, 24, 28, and 32 and *Helwig et al.*'s system that contradict the factual determination that *Helwig et al.* identically describe the claimed invention within the meaning of 35 USC §102.

With respect to claim 1, there is no teaching or suggestion within *Helwig et al.* of:

a) establishing a communications channel in which there is then established "a first stream between the first process and the communication channel"; and

b) "establishing a second stream between the second process and the communication channel"; and

c) encrypting, independent of a transport protocol, data in response to the data being written to the first stream; and

d) decrypting, independent of the transport protocol, the encrypted data in response to the encrypted data being read form the second stream.

In addition to the features identified above with respect to claim 1, claim 5 recites a computer-readable medium, carrying code that when executed performs various functions. This requirement of claim 5 is not disclosed by *Helwig et al.*

In addition to the features identified above with respect to claim 1, claim 13 recites a computer data signal embodied on a carrier wave, representing instructions that when executed performs various functions. This requirement of claim 13 is not disclosed by *Helwig et al.*

With respect to claim 17, there is no teaching or suggestion within *Helwig et al.* of:

a) establishing a stream between a process and a communication channel; and

b) encrypting data independent of communication protocol layers in response to data being written to the stream.

With respect to claim 20, there is no teaching or suggestion in *Helwig et al.* of:

a) establishing a first stream from a first process to the communication channel; and

b) establishing a second stream from the communication channel to a second process.

In addition to the features identified above with respect to claim 20, claim 24 recites a computer-readable medium, carrying code that when executed performs various functions. This requirement of claim 24 is not disclosed by *Helwig et al.*

In addition to the features identified above with respect to claim 20, claim 28 recites a communications network performing the recited method steps. This requirement of claim 28 is not disclosed by *Helwig et al.*

In addition to the features identified above with respect to claim 20, claim 32 recites a computer data signal embodied on a carrier wave, representing instructions that when executed performs various functions. This requirement of claim 32 is not disclosed by *Helwig et al.*

The above argued differences between the claimed inventions and the system of *Helwig et al.* undermine the factual determination that *Helwig et al.* identically describe the claimed inventions within the meaning of 35 USC §102. **Kolster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 230 USPQ 81 (Fed. Cir. 1986). Thus, the Examiner has failed to establish a prima facie case of anticipation.** Appellants, therefore, respectfully submit that each the imposed rejection of claims 1, 5, 13, 17, 20, 24, 28 and

32 under 35 USC §102 for lack of novelty, as evidenced by *Helwig et al.*, are independently factually erroneous.

**B. The Examiner erred in rejecting claims 1, 5, 13, 17, 20, 24, 28 and 32 as anticipated by Schneier.**

The Examiner erred in rejecting claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(b) as anticipated by *Schneier* (Applied Cryptography). The factual determination that *Schneier* identically disclose the claimed inventions recited in claims 1, 5, 13, 17, 20, 24, 28, and 32 under 35 USC §102(b) is erroneous given the differences between the claimed inventions and the system of *Schneier*. *Schneier* describes an XOR encryption process, known as a stream cipher, with its corresponding decryption process. With respect to all the claims, this discussion of a ciphering model by *Schneier* does not disclose (or even suggest) establishment of a communications channel followed by establishing a stream between a process and the channel and another stream from the channel to an output process. Thus, the Examiner has failed to establish a *prima facie* case of anticipation.

With respect to claim 1, there is no teaching or suggestion within *Schneier* of:

a) establishing a communications channel in which there is then established "a first stream between the first process and the communication channel"; and

b) "establishing a second stream between the second process and the communication channel"; and

c) encrypting, independent of a transport protocol, data in response to the data being written to the first stream; and

d) decrypting, independent of the transport protocol, the encrypted data in

response to the encrypted data being read form the second stream.

In addition to the features identified above with respect to claim 1, claim 5 recites a computer-readable medium, carrying code that when executed performs various functions. This requirement of claim 5 is not disclosed by *Schneier*

In addition to the features identified above with respect to claim 1, claim 13 recites a computer data signal embodied on a carrier wave, representing instructions that when executed performs various functions. This requirement of claim 13 is not disclosed by *Schneier*

With respect to claim 17, there is no teaching or suggestion within *Schneier* of:

a) establishing a stream between a process and a communication channel; and

b) encrypting data independent of communication protocol layers in response to data being written to the stream.

With respect to claim 20, there is no teaching or suggestion in *Schneier* of:

a) establishing a first stream from a first process to the communication channel; and

b) establishing a second stream from the communication channel to a second process.

In addition to the features identified above with respect to claim 20, claim 24 recites a computer-readable medium, carrying code that when executed performs various functions. This requirement of claim 24 is not disclosed by *Schneier.*

In addition to the features identified above with respect to claim 20, claim 28 recites a communications network performing the recited method steps. This requirement of claim 28 is not disclosed by *Schneier*

In addition to the features identified above with respect to claim 20, claim 32

recites a computer data signal embodied on a carrier wave, representing instructions that when executed performs various functions. This requirement of claim 32 is not disclosed by *Schneier*

The above argued differences between the claimed inventions and the system of *Schneier* undermine the factual determination that *Schneier* identically describe the claimed inventions within the meaning of 35 USC §102. **Kolster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 230 USPQ 81 (Fed. Cir. 1986).**

**Thus, the Examiner has failed to establish a prima facie case of anticipation.** Appellants, therefore, respectfully submit that each the imposed rejection of claims 1, 5, 13, 17, 20, 24, 28 and 32 under 35 USC §102 for lack of novelty, as evidenced by *Schneier*, are independently factually erroneous.

**C. The factual determination that either *Helwig et al.* or *Schneier* identically disclose (or even suggest) a "stream" as meant and recited in <u>any</u> of the present claims is erroneous when the appropriate disclosures are considered as a whole and interpreted with internal consistency and from the perspective of one of ordinary skill.**

Neither *Helwig et al.* nor *Schneier* teach or suggest the use of a "stream" as that term was used or applied in the specification and claims of the present application.

<u>*Helwig et al.*:</u>

*Helwig et al.* does refer to a "data stream" However, the use of similar <u>sounding</u> terms is not necessarily the same as using terms that <u>mean</u> the same thing. Therefore, the mere use of similar sounding terms does not end the inquiry into whether a reference can be considered as identically disclosing the same subject matter. The meaning of "data streams" in *Helwig et al.* is interpreted in the context of that specification and within

*Helwig et al.* the "data streams" are a series of bits output from a vocoder and are used as a description of the data's particular physical format.

In contrast to the interpretation as meant by *Helwig et al.*, the present claim term "stream" is to be interpreted in light of the claim language, the specification, and the prosecution history; and the interpretation proceeds from the vantage point of one skilled in the art. **Atlantic Thermoplastics Co., Inc. v. Faytex Corp., 970 F.2d 834, 23 USPQ2d 1481 (Fed. Cir. 1992); Haynes International, Inc. v. Jessop Steel Co., 8 F.3d 1573, 28 USPQ2d 1652 (Fed. Cir. 1993).** Ultimately, claim language is construed according to the standard of what those words would have meant to one skilled in the art as of the application date. **Weiner v. NEC Electronics, Inc., 102 F.3d 534, 41 USPQ2d 1023 (Fed. Cir. 1996).**

It is important to interpret the phrase "stream" within the claims in a way which is consistent with the specification, rather than at odds to it. For example, one would obviously not interpret "stream" in the context of this application as referring to a flow of water down a mountain side. On page 4 of the specification, beginning line 9, the application introduces a "stream" as an abstraction which refers to the transfer or "flow" of data, in any format, from a single source, to a single destination. Let us consider the following example in the context of Figure 1 of the application. Let us assume that process 108 is an MPEG2 transmission process. It may generate a plurality of "streams", such as a left channel audio, a right channel audio, a video, a closed-captioned stream, and a control channel stream. When the MPEG2 transmission process 108 desires to send information to process 110, which, in this example, is an MPEG2 display process, a communications channel would be set up between node 108 and node 104 then, the individual streams

would be applied to the communications channel for transmission to the node 104. Note that the communication channel from the process 108 goes through all of the layers shown in Figure 1 of each protocol stack, namely the application layer, presentation layer, session layer, transport layer, network layer, datalink layer, and physical layer before going across the transmission medium to the other node and then passing through the same layers as an inverse order. It is known in the art to apply layer specific encryption at any of the layers of the OSI reference model shown in Figure 1.

If the invention of claim 1 were applied to a communication system which corresponded to the OSI reference model, first, communications would be established between the first network node and the second network node. The request for connection would come from the process 108 to the application layer and appropriately process through the layers until a connection is set up to node 104. Once that is done, a first stream, say, for example, an MPEG control channel stream is established between the first process 108 and the communications channel which begins at application layer 118. At the other end, a stream would be established between the application layer 128 of node 104 and the process 110 for the MPEG control channel data. As set forth in limitation d) of claim 1, in response to data being written to the first stream [from process 108] the data is encrypted to generate encrypted data which is then applied to the application layer 118. The encryption is performed independently of any of the layers of the communications protocol stack. Note that in the example of MPEG2, encryption can be applied selectively to the streams rather than to everything that is transmitted over the communications channel. In OSI reference model, the layer normally responsible for encryption is the presentation layer while the application layer, 118, handles the interface between the

software involved with the process 108 and the communications channel.

One limitation of claim 1 states "in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover the decrypted data."

As used within the present application, "stream" is an abstraction, which has properties beyond merely being a string of binary digits. "Streams", as would be understood by a skilled software practitioner, are defined in object oriented languages such as Java and have a whole set of associated properties which distinguish them from a flow of water down the mountain side and which also distinguish them from simply an arbitrary string of binary 1's and 0's.

*Schneier*:

With regards to *Schneier*, the referenced portion (Section 9.4) of his book **Applied Cryptography** describes a cipher model known as "Stream Ciphers". In particular, the Examiner relies of Figure 9.6 as anticipating the present claims. So, similar to Helwig et. al., *Schneier* also uses a similar sounding term -- "stream cipher"; but, once again, the inquiry is not whether similar sounding terms are being used but whether the terms being used convey an identical disclosure of subject matter as required under 35 USC §102.

The following information from **Ritter's Crypto Glossary and Dictionary of Technical Cryptography** (Current Edition: 2002 Feb 18, which can be found at, for example, http://www.ciphersbyritter.com/GLOSSARY.HTM)provides a helpful context for evaluating the disclosure of *Schneier*.

The glossary has a heading of "Cipher Taxonomy" which includes the following

definitions:

> **BLOCK CIPHER**
> A block cipher requires the accumulation of some amount of data or multiple data elements for ciphering to complete. (Sometimes stream ciphers accumulate data for convenience, as in cylinder ciphers, which nevertheless logically cipher each character independently.)
>
> **STREAM CIPHER**
> A stream cipher does not need to accumulate some amount of data or multiple data elements for ciphering to complete. (Since we define only two main "types" of cipher, a stream cipher is the opposite of a block cipher and vise versa. It is extremely important that the definitions for block and stream ciphering enclose the universe of all possible ciphers.) A stream cipher has the ability to transform individual elements one-by-one. The actual transformation usually is a block transformation, and may be repeated with the same or different keying.

A later heading in this Glossary that relates to a "Stream Cipher" further agrees with the specific XOR implementation of *Schneier* by describing a stream cipher as:

> a cipher which directly handles messages of arbitrary size by ciphering individual data elements, such as bits or bytes or characters. Conventionally, some form of keyed random number generator is used to produce a confusion sequence or running key. That sequence is then combined with plaintext data by exclusive-OR to produce ciphertext. Enciphering individual characters allows ciphering to begin immediately, avoiding the need to accumulate a full block of data before ciphering, as is necessary in a conventional block cipher. But note that a stream cipher can be seen as an operating mode, a "streaming" of a tiny block transformation. Stream ciphers can be called "combiner-style" ciphers. Also see: a cipher taxonomy.

Appellants urge that the high-level discussion of a stream ciphering model by *Schneier* does not provide the requisite identical disclosure of the "stream" abstraction as intended and used in the present specification and claims.

Thus, the Examiner has failed to establish a *prima facie* case of anticipation of the

claims when the claims, *Schneier* and *Helwig et al.* are all properly interpreted, because such an interpretation reveals that neither of the references identically disclose the "stream" recited in the claims.

**D. The Examiner erred in rejecting claims 3, 4, 7, 8, 15, 16, 18, 19, 22, 23, 26, 27, 29, 30, 31, 34, and 35 as unpatentable over either Helwig et al. or Schneier.**

Claims 3, 4, 7, 8, 15, 16, 18, 19, 22, 23, 26, 27 [and 29], 30, 31, 34 and 35 are not obvious over either *Helwig et al.* or *Schneier* because neither of these references teach or other wise suggest a Java-based stream or communication channel and, thus, the Examiner did not discharge the initial burden of establishing a prima facie basis to deny patentability to the claimed invention under 35 USC §103.

In applying these references to the claims, the Examiner states:

> "They do not say that the communication channels or data streams are Java-based. Official notice is taken that it is old and well-known that Java is intended for networked/distributed environments and enables the construction of virus-free, tamper-free systems. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to base the systems of *Schneier* or *Helwig et al.*, all of which are networked or distributed environments, on Java, as is known in the art. This would enable the implementation of a virus-free, tamper-free system."

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision always rests upon the Examiner. **In re Mayne, 41 USPQ2d 1451 (Fed .Cir. 1997); In re Deuel, 34 USPQ2d 1210 (Fed. Cir. 1995); In re Bell, 26 USPQ2d 1529 (Fed. Cir. 1993); In re Oetiker, 24 USPQ2d 1443 (Fed. Cir. 1992).** In rejecting a claim under 35 U.S.C. § 103, the Examiner is required to provide a factual basis to support the obviousness conclusion. **In re Warner, 154 USPQ 173 (CCPA 1967); In re Lunsford, 148 USPQ 721 (CCPA 1966); In re Freed,**

**165 USPQ 570 (CCPA 1970).** The Examiner is required to show that all the claim limitations are taught or suggested by the references along with some motivation to combine the teachings of the references. **In re Royka, 180 USPQ 580 (CCPA 1974); In re Wilson, 165 USPQ 494 (CCPA 1970).**

In addition, it has been repeatedly held by the Court of Appeals for the Federal Circuit that in order to establish the requisite realistic motivation, the Examiner must make "clear and particular" factual findings as to a specific understanding or specific technological principle which would have realistically impelled one having ordinary skill in the art to modify a particular prior art device (the device of either *Schneier* or *Helwig et al.*) to arrive at the claimed invention based upon facts--not generalizations. **Ruiz v. A.B. Chance Co., 234 F.2d 654, 57 USPQ2d 1161 (Fed. Cir. 2000); Ecolochem Inc. v. Southern California Edison, Co. 227 F.3d 361, 56 USPQ2d 1065 (Fed. Cir. 2000); In re Kotzab, 217 F.3d 1365, 55 USPQ 1313 (Fed. Cir. 2000); In re Dembiczak, 175 F.3d 994, 50 USPQ2d 1614 (Fed. Cir. 1999).** Moreover, the Examiner is required to explain **why** one having ordinary skill in the art would have been realistically led to modify the devices of either *Schneier* or *Helwig et al.* to arrive at the claimed invention. **Ecolochem Inc. v. Southern California Edison, Co. supra.; In re Rouffet, 149 F.3d 1350, 47 USPQ2d 1453 (Fed. Cir. 1998).** Significantly, the requisite motivation must be undertaken with a reasonably expectation of successfully achieving the objective of either *Schneier* or *Helwig et al.* **In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).**

Appellant would heavily rely upon the legal tenet that regardless of what the Examiner perceives as the source of motivation in the prior art, the Examiner must

provide "a convincing discussion of the specific sources of the motivation to combine the prior art references...". **Ecolochem Inc. v. Southern California Edison, Co. 227 F.3d 1361, 56 USPQ2d 1065 (Fed. Cir. 2000)**. This basis legal tenet was recently enforced by the Court of Appeals for the Federal Circuit in **In re Lee ____F.3d ____, 61USPQ2d 1430 (Fed. Cir. 2002)**, wherein the Court emphasized that the motivational element is a factual question which requires substantial evidence--not conclusory statements.

Appellants continue to insist that the range and content of the Examiner's Official Notice is factually and legally erroneous. But, assuming for the sake of argument that the Official Notice was effective for what the Examiner asserts, Appellants urge that the requirements of 35 USC §103 have still not been satisfied. The Examiner has failed to provide a cogent explanation of why one of ordinary skill would have been motivated to modify the message storing device of to *Helwig et al.* to add, for example, the complexity, additional hardware and cost of Java processing capability in the first place. Additionally, the Examiner has failed to provide a cogent explanation of why one of ordinary skill would have been motivated to augment the general discussion of enciphering and deciphering models by *Schneier* to specifically involve Java and Java streams. The Examiner states that Java "enables construction of virus-free, tamper-free systems". This type of generalization about technology is exactly the danger of which the courts have repeatedly warned against and the type of reasoning which the courts have repeatedly found erroneous. The establishment of a prima facie case of obviousness must factually explain why one of ordinary skill would have been motivated to combine specific teachings, in a specific way in order to arrive at a specific invention.

The Examiner's Official Notice (even if true) that Java might have use in tamper-free systems, is not a factual explanation of why a skilled artisan would have found it obvious to modify the specific systems taught by *Schneier* or *Helwig et al.* with some reasonable expectation of success.

If the Examiner were to implement the *Schneier* or *Helwig et al.* systems, using Java streams and Java secure channels, it would still not result in the claimed invention. In fact, if the phrases "communication channel" and "stream" as used in each of the references are interpreted to be a "Java stream" and "Java secure communication channel," the interpretation of the references as applied to the independent claims would have to change so dramatically as to show their inapplicability under 35 USC §102.

Appellants urge that the Examiner committed clear factual and legal errors. Specifically, without the benefit of any facts, the Examiner expanded the teachings of the applied references to whatever level he needed in order to combine them, relying only upon his "official notice" ability, in complete violation of **Ex parte Stern, 13 USPQ2d 1379 (BPAI 1987).**

Appellants recognize that the specific limitations recited in the different "families" of dependent claims appear to be very similar. However, as the patentability of each of the independent claims was separately argued, Appellants wish to stress that the dependent claims also stand or fall individually and are not being grouped together.

With respect to claim 3, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 3 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 4, the claim recites a first Java stream, a second Java stream,

a third Java stream, and a Java secure channel. These requirements of claim 4 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 7, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 7 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 8, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 8 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 15, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 15 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 16, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 16 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 18, the claim recites a first Java stream and a Java secure channel. These requirements of claim 18 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 19, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 19 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 22, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 22 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 23, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 23 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 26, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 26 are not disclosedor suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 27, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 27 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 29, the claim recites that the encryption of the first stream and the decryption of the second stream is specific to a communication protocol layer. This requirement of claim 29 is not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 30, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 30 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 31, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 31 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 34, the claim recites a first Java stream, a second Java stream, and a Java secure channel. These requirements of claim 34 are not disclosed or suggested by either *Helwig et al.* or *Schneier.*

With respect to claim 35, the claim recites a first Java stream, a second Java stream, a third Java stream, and a Java secure channel. These requirements of claim 35 are not

disclosed or suggested by either *Helwig et al.* or *Schneier.*

The above argued differences between the claimed inventions and the system of *Helwig et al.* and *Schneier* undermine the factual determination that *Helwig et al.* and *Schneier* provide a prima facie case of obviousness within the meaning of 35 USC §103 of claims 3, 4, 7, 8, 15, 16, 18, 19, 22, 23, 26, 27, 30, 31, 34 and 35

**E. The Examiner erred in rejecting claims 2, 6, and 14 as unpatentable over either Helwig et al. or Schneier.**

Claims 2, 6, and 14 are not obvious over either *Helwig et al.* or *Schneier* because neither of these references teach or other wise suggest performing communication protocol layer specific encryption or decryption of the data and, thus, the Examiner did not discharge the initial burden of establishing a prima facie basis to deny patentability to the claimed invention under 35 USC §103.

In rejecting these claims, the Examiner asserts that if some encryption is good, then more encryption is better. Appellants admit that some liberty was taken with paraphrasing the Examiner's comments; however, if read carefully, his assertions really do not say anything more than the above generalization. As stated previously, the Examiner must make "clear and particular" factual findings as to a specific understanding or specific technological principle which would have realistically impelled one having ordinary skill in the art to modify a particular prior art device (the device of either *Schneier* or *Helwig et al.*) to arrive at the claimed invention based upon facts--not generalizations.

Each of claims 2, 6 and 14 require more than simply a second encryption step. The claims recite that the encryption being performed be "a communication protocol

layer specific encryption." The Examiner has not explained why a skilled artisan, with either *Schneier* or *Helwig et al.* in hand, would have found it obvious to add to the respective systems a communication layer protocol specific encryption. *Schneier* does not disclose a stream cipher in the context of networked nodes communicating over a channel and *Helwig et al.* is concerned about storing a message, not with secure communications. Additionally, *Helwig et al.* discusses the need for responsiveness in their system and one skilled in the art would not have adversely impacted performance in such a system by adding another layer of encryption processing. Accordingly, the Examiner's generalization might indicate that employing multiple layers of encryption was known and even that protocol specific encryption was known. However, these conclusions fall far short of establishing a prima facie case of obviousness under 35 USC §103. The Examiner has failed to provide a fact-based rationale why one of ordinary skill would have been motivated to modify specifically *Schneier* or *Helwig et al.* with a second encryption/decryption step and why that skilled artisan would have performed the encryption/decryption as being protocol layer specific.

The lack of a fact-based explanation for expanding the teachings of *Helwig et al.* and *Schneier* undermine the factual determination that *Helwig et al.* and *Schneier* provide a prima facie case of obviousness within the meaning of 35 USC §103 of claims 2, 6, and 14.

**F. Claims 2, 3, 4, 6, 7, 8, 14, 15, 16, 18, 19, 22, 23, 26, 27 [and 29], 30, 31, 34 and 35 are not obvious over either *Helwig et al.* or *Schneier* because neither of these references anticipate the respective independent claims from which these claims depend and, thus, the Examiner did not discharge the initial burden of establishing a prima facie basis to deny patentability to the claimed invention under 35 USC §103.**

In rejecting the dependent claims, the Examiner relies on either *Helwig et al.* or *Schneier* as applied to the independent claims and then asserts, through "Official Notice" that the specific features in the dependent claims are well-known.

As argued above, neither of the applied references disclose all the features of the independent claims -- features which are incorporated into respective dependent claims. Accordingly, for the reasons presented above, with regard to the independent claims, neither reference discloses or suggests every feature recited in the dependent claims.

Neither *Schneier* nor *Helwig et al.*, therefore, provide the factual basis needed to properly establish a prima facie case of obviousness under 35 USC §103.

## CONCLUSION

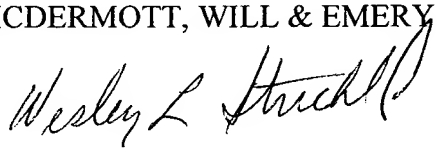
For the reasons advanced above, the Examiner's factual determination that *Schneier* identically describes the claimed inventions of claims 1, 5, 13, 17, 20, 24, 28 and 32, within the meaning of 35 USC §102, is erroneous. For the reasons advanced above, the Examiner's factual determination that *Helwig et al.* identically describe the claimed inventions of claims 1, 5, 13, 17, 20, 24, 28 and 32, within the meaning of 35 USC §102, is erroneous. Appellants, therefore, respectfully solicit the Honorable Board to **reverse** each of the Examiner's rejections.

For the reasons advanced above, Appellants submit that the Examiner did not establish a *prima facie* basis to deny patentability to any of the claims on Appeal under 35 USC §103. Appellants, therefore, respectfully solicit the Honorable Board to **reverse** each of the Examiner's rejections under 35 USC §103.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-0417 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Wesley L. Strickland
Registration No. 44,363

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 WLS:cac
**Date: March 25, 2002**
Facsimile: (202) 756-8087

APPENDIX

1. (Twice Amended) A method for providing communication protocol layer independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, wherein the first network node and the second network node each support at least one common communication protocol layer, the method comprising the steps of:

establishing a communication channel between the first network node and the second network node;

establishing a first stream between the first process and the communication channel;

establishing a second stream between the second process and the communication channel;

in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node;

causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of

the encrypted data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node.

2. (Thrice Amended) The method of Claim 1, further including the steps of

performing a communication protocol layer specific encryption of the data on the first network node, and

performing a communication protocol layer specific decryption of the data on the second network node.

3. The method of Claim 1, wherein the communication channel is a Java secure channel,

wherein the first stream is a first Java stream,

wherein the second stream is a second Java stream,

wherein the step of establishing a communication channel between the first and second network nodes further comprises the step of establishing a Java secure channel between the first and second network nodes,

wherein the step of establishing a first stream between the first process and the communication channel further comprises the step of establishing a first Java stream between the first process and the Java secure channel, and

wherein the step of establishing a second stream between the second process and the communication channel further comprises the step of establishing a second Java stream between the second process and the Java secure channel.

4. (Twice Amended) The method of Claim 1, wherein the communication channel is a Java secure channel, wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the method further comprises the step of connecting the Java secure channel to a third Java stream, and

wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

5. (Twice Amended) A computer-readable medium carrying one or more sequences of one or more instructions for providing communication protocol layer independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, wherein the first network node and the second network node each support at least one common communication protocol layer, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

establishing a communication channel between the first network node and the second network node;

establishing a first stream between the first process and the communication channel;

establishing a second stream between the second process and the communication channel;

in response to the data being written to the first stream, encrypting the data to

generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node;

causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node.

6. (Twice Amended) The computer-readable medium of Claim 5, wherein the computer-readable medium further includes instructions for performing the steps of

performing a communication protocol layer specific encryption of the data on the first network node, and

performing a communication protocol layer specific decryption of the data on the second network node.

7. The computer-readable medium of Claim 5, wherein the first stream is a first Java stream,

wherein the second stream is a second Java stream,

wherein the step of establishing a communication channel between the first and

second network nodes further comprises the step of establishing a Java secure channel between the first and second network nodes,

wherein the step of establishing a first stream between the first process and the communication channel further comprises the step of establishing a first Java stream between the first process and the Java secure channel, and

wherein the step of establishing a second stream between the second process and the communication channel further comprises the step of establishing a second Java stream between the second process and the Java secure channel.

8. (Amended) The computer-readable medium of Claim 5, wherein the communication channel is a Java secure channel,

wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the computer-readable medium further includes instructions for connecting the Java secure channel to a third Java stream, and

wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

13. (Twice Amended) A computer data signal embodied in a carrier wave and representing sequences of instruction which, when executed by one or more processors, provide communication protocol layer independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, according to at least one common communication protocol layer

supported by the first and second network nodes, by performing the steps of:

establishing a communication channel between the first network node and the second network node;

establishing a first stream between the first process and the communication channel;

establishing a second stream between the second process and the communication channel;

in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node;

causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node.

14. (Twice Amended) The computer data signal of Claim 13, wherein the computer sequence of instructions further includes instructions for performing the steps of

performing a communication protocol layer specific encryption of the data on the first network node, and

performing a communication protocol layer specific decryption of the data on the second network node.

15. The computer data signal of Claim 13, wherein the first stream is a first Java stream,

wherein the second stream is a second Java stream,

wherein the step of establishing a communication channel between the first and second network nodes further comprises the step of establishing a Java secure channel between the first and second network nodes,

wherein the step of establishing a first stream between the first process and the communication channel further comprises the step of establishing a first Java stream between the first process and the Java secure channel,

wherein the step of establishing a second stream between the second process and the communication channel further comprises the step of establishing a second Java stream between the second process and the Java secure channel.

16. (Amended) The computer data signal of Claim 13, wherein the communication channel is a Java secure channel,

wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the computer sequence of instructions further includes instructions for

connecting the Java secure channel to a third Java stream, and

wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

17. (Amended) A method for providing communication protocol layer independent security for data transmitted by a process executing on a network node, the method comprising the steps of:

a) establishing a stream between the process and a communication channel; and

b) in response to the data being written to the stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data on the communication channel.

18. (Amended) The method of Claim 17, wherein the communication channel is a Java secure channel,

wherein the stream is a first Java stream, and

wherein the step of establishing a stream between the process and the communication channel further comprises the step of establishing a Java stream between the process and the Java secure channel.

19. (Amended) The method of Claim 17, wherein the communication channel is a Java secure channel, wherein the stream is a Java stream,

wherein the method further comprises the step of connecting the Java secure channel to a second Java stream, and

wherein the second Java stream provides for the transmission of data according to a specific communication protocol layer.

20. (Amended) A method for providing communication protocol-independent security for data transmitted between a first node and a second node, the method comprising the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel after the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process after the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

22. (Amended) The method of claim 20, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node

and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

23. (Amended) The method of claim 20, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream;

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

24. (Amended) A computer-readable medium carrying one or more sequences of one or more instructions for providing communication protocol-layer independent security for data transmitted between a first node and a second node, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel after the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process after the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

26. (Amended) The computer-readable medium of claim 24, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

27. The method of claim 24, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

28. (Amended) A communications network providing communication protocol-independent security for data transmitted between a first node and a second node, the communication network performing the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel after the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process after the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

29. The communication network of claim 28, wherein the encryption of the first stream and the decryption of the second stream is specific to a communication protocol layer.

30. (Amended) The communication network of claim 28, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

31. The communication network of claim 28, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

32. (Amended) A computer data signal embodied in a carrier wave and representing sequences of instructions which, when executed by one or more processor, provide communication protocol-independent security for data transmitted between a

first node and a second node, by performing the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel after the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process after the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

34. (Amended) The computer data signal of claim 32, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

35. The computer data signal of claim 32, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.